REGOLAMENTO PER L'UTILIZZO DELLE RISORSE INFORMATICHE DELL'UNIVERSITÀ DEGLI STUDI DEL MOLISE

Articolo 1

Finalità e ambito di applicazione

Il presente Regolamento stabilisce le condizioni e le modalità vincolanti per l'accesso e l'utilizzo delle risorse informatiche e della Rete Informatica e Telematica dell'Università degli Studi del Molise, in seguito indicata come Rete dati di Ateneo.

L'Università degli Studi del Molise, consapevole delle potenzialità offerte dagli strumenti informatici e telematici, promuove l'utilizzo della Rete Dati di Ateneo, quale strumento utile, sempre compatibilmente con le proprie strutture e risorse, esclusivamente a perseguire le proprie finalità nel quadro dell'attività istituzionale e amministrativa, della didattica e della ricerca.

Articolo 2

Definizioni

Ai fini del presente Regolamento, si intendono adottate le definizioni seguenti:

- *Coordinamento Servizi Informatici, Telematici e Multimediali (CSITEM)*: struttura preposta alla gestione tecnica dei servizi informatici, telematici e multimediali suddivisa in SISRA (Settore Sistemi Informativi, Servizi di Rete ed Assistenza), SIM (Settore Servizi Interni e Multimediali) e PPSS (Settore Programmazione, Progettazione e Servizi Strategici);
- *Credenziali di accesso*: dati utilizzati nelle operazioni di autenticazione utente (per es. nome utente e password);
- *Firma elettronica qualificata*: firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro (ad es: smart card) per la creazione della firma;
- *Firma digitale*: particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;
- *GARR*: Gruppo Armonizzazione Reti per la Ricerca;
- *Host (terminale informatico)*: ogni computer, stampante, periferica, telefono, fax o qualsiasi dispositivo informatico, di proprietà dell'Università degli Studi del Molise (o non di proprietà solo se autorizzati), connesso alla Rete Dati di Ateneo ad una Presa utente interna;
- *IP (Internet Protocol)*: numero che identifica univocamente un host nella Rete Dati di Ateneo;
- *Log:* file o insieme di file contenenti le registrazioni di operazioni compiute durante l'utilizzo di un servizio di rete nonché la registrazione dei dati necessari all'identificazione dei responsabili di tali operazioni;

- *Posta Elettronica Certificata (PEC)*: è un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici;
- *Presa utente interna*: punto di connessione fonia/dati (nodo terminale), al quale può essere collegato un Host;
- *Rete dati di Ateneo*: insieme delle infrastrutture fisiche e logiche che consentono la comunicazione e la trasmissione dati e fonia sia all'interno che all'esterno dell'Ateneo.
- *Servizi in rete*: servizi che utilizzano la Rete Dati di Ateneo e che sono erogati da alcune strutture dell'Ateneo a beneficio dell'amministrazione centrale, della didattica e della ricerca (accesso ad Internet, controllo di gestione economica, telefonia VoIP- Voice over Internet Protocol, posta elettronica, protocollo informatico, servizi di segreteria, sistema di rilevazione e gestione presenze dei dipendenti, sistema contabilità, sito web di Ateneo…);
- *Struttura d'Ateneo*: complesso edilizio autonomo;
- *Utente*: qualsiasi persona o struttura autorizzata che accede ai servizi in rete dell'Università degli Studi del Molise.

Articolo 3

Utenti con accesso alla Rete dati di Ateneo

Gli utenti che hanno facoltà di accesso alla Rete dati di Ateneo sono i professori e i ricercatori dell'Università, il personale tecnico-amministrativo, gli studenti regolarmente iscritti all'Università o a corsi e seminari, convegni gestiti o organizzati dall'Università anche in compartecipazione con altri enti con i quali esistano apposite convenzioni, i dottorandi di ricerca, i titolari di borse post-dottorato, i titolari di borse e/o contratti di ricerca, i collaboratori alla ricerca, i componenti degli organi dell'Università ancorché non dipendenti dell'Università.

Possono accedere alla Rete dell'Università per il periodo di tempo necessario all'espletamento dei loro compiti all'interno dell'Ateneo i docenti a contratto, i collaboratori e i ricercatori esterni impegnati in attività da svolgersi all'interno dell'Università e a coloro ai quali è consentito l'accesso da regolamenti di altre strutture dell'Ateneo; per tutti questi casi dovrà essere esplicitamene indicato il nominativo del referente interno dell'Ateneo (coordinatore del progetto, docente titolare dell'attività di ricerca, etc).

Convenzioni di Ricerca tra l'Ateneo ed altri Enti pubblici o privati possono prevedere un utilizzo delle risorse della rete d'Università limitatamente agli appartenenti agli Enti in questione che partecipino alle attività oggetto delle convenzioni, e per le attività ad esse relative. L'accesso in ambito convenzionale alla rete d'Università deve comunque essere regolamentato da un documento tecnico che ne specifica in dettaglio le condizioni, approvato e sottoscritto dai responsabili tecnici e amministrativi delle parti in questione e allegato alla convenzione stessa.

Potrà essere autorizzato, caso per caso, l'accesso a singoli Utenti che non rientrano nelle categorie sopraelencate.

Articolo 4

Modalità di connessione degli Host alla Rete dati di Ateneo

Per poter connettere un qualunque Host in Rete il Referente informatico di struttura o l'Utente, deve ottenere una specifica autorizzazione dal SISRA che rilascerà appositi dati di configurazione tra cui l'indirizzo IP. Il SISRA può rendere necessario, per la connessione dell'Host alla rete, l'utilizzo delle

credenziali di cui al successivo articolo 5.
La richiesta di accesso alla Rete Dati di Ateneo deve essere inoltrata al SISRA utilizzando l'apposita modulistica disponibile sul Sito Web di Ateneo www.unimol.it.
Per gli Host, non di proprietà dell'Università, è necessario che l'utente richieda, tramite le relative strutture amministrative di riferimento, l'autorizzazione, anche se temporanea, all'accesso alla rete dati di Ateneo.
Nella richiesta di accesso alla Rete dati di Ateneo, qualora il sistema informatico in rete eroghi servizi, questi dovranno essere debitamente dichiarati.

Articolo 5

Credenziali di accesso alla Rete dati di Ateneo

Gli utenti con facoltà di accesso alla Rete dati di Ateneo hanno diritto a richiedere tramite le relative strutture amministrative di riferimento (ad esempio, i docenti al Settore Docente, il personale tecnico-amministrativo al Settore Personale Tecnico-amministrativo, gli studenti alla Segreteria Studenti…) le credenziali di accesso per poter utilizzare determinati servizi in rete.
L'utente è tenuto a conservare con diligenza le credenziali di accesso ai servizi avendo cura che esse non vengano utilizzate in modo improprio. L'utente dovrà prontamente avvisare il CSITEM nell'ipotesi di smarrimento o anche di probabile diffusione presso terzi dei dati di accesso.
L'utilizzo delle credenziali di accesso ai servizi informatici sarà registrato in appositi file (Log) per gli usi consentiti dalla legge e dal presente regolamento.
L'uso delle credenziali è strettamente personale: ogni attività non regolare verrà imputata, nei limiti di legge, al titolare.

Articolo 6

Posta elettronica

L'Università degli Studi del Molise, nell'ambito delle proprie attività, ferma restando l'osservanza delle norme in materia della riservatezza dei dati personali e delle norme tecniche di sicurezza informatica, si adopera per estendere la diffusione e l'utilizzo degli strumenti telematici in sostituzione dei canali tradizionali di comunicazione.
A tal fine agli utenti che abbiano ottenuto l'accesso alla Rete dati di Ateneo dell'Università degli Studi del Molise viene riconosciuta la possibilità di disporre di almeno una casella postale personale (anche per coloro i quali non sia prevista la dotazione di un personal computer).
IL SISRA può attivare anche apposite caselle istituzionali affidate alla responsabilità delle strutture di competenza. Gli utenti dovranno procedere alla tempestiva lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta, adottando gli opportuni metodi di conservazione della stessa in relazione alle varie tipologie di messaggi ed ai tempi di conservazione richiesti.
La posta elettronica può essere utilizzata per la trasmissione di tutti i tipi di informazioni, documenti e comunicazioni in formato elettronico e, a differenza di altri mezzi tradizionali, offre notevoli vantaggi in termini di maggiore semplicità ed economicità di trasmissione, inoltro e riproduzione.
Inoltre, il SISRA dispone di caselle di posta elettronica certificata, efficace strumento per la trasmissione dei documenti informatici ai sensi della disciplina vigente in materia di firme digitali ed elettroniche certificate.
L'Amministrazione si riserva di effettuare i necessari controlli su eventuali utilizzi, consapevolmente

impropri del servizio, ricorrendo, ove necessario, alle autorità competenti.

Articolo 7

Responsabilità e obblighi dell'utente

L'utilizzo dei servizi della Rete dati di Ateneo e delle risorse informatiche è subordinato al rispetto da parte dell'utente della normativa vigente, del presente Regolamento, oltre che delle norme che regolano la Rete GARR e che costituiscono parte integrante del presente Regolamento nel loro ambito di applicazione (Allegato A).

Pertanto l'utente, otterrà l'autorizzazione all'utilizzo dei servizi della Rete dati di Ateneo, solo dopo essersi impegnato, tramite esplicito e formale consenso espresso nell'apposito modulo:

- ad osservare il presente Regolamento;
- a rispettare la normativa vigente, le norme GARR ed eventuali altre regole che disciplinano le attività e i servizi che utilizzano la Rete dati di Ateneo;
- ad acconsentire al trattamento dei suoi dati personali e dei log da parte dell'Ateneo, in conformità alle norme legislative e regolamentari vigenti.

Si sottolinea che:

- l'utente interno è responsabile delle attività svolte nella Rete dati di Ateneo;
- l'utente è responsabile per eventuali difformità riscontrate sulle apparecchiature assegnate;
- la modifica dell'indirizzo IP è espressamente vietata;
- le credenziali di accesso sono personali e non possono essere condivise o cedute;
- l'utente è responsabile per la protezione dei dati utilizzati e/o memorizzati nei sistemi a cui ha accesso ed è tenuto ad adottare tutte le misure necessarie ai sensi della normativa vigente e del documento programmatico di sicurezza dell'Ateneo (utilizzo di password, backup dati…);
- l'utente è tenuto a mantenere aggiornato il software antivirus installato sull'Host utilizzato;
- la responsabilità del contenuto dei materiali prodotti e diffusi attraverso la rete è dell'utente che li produce e li diffonde;
- l'utente è obbligato a segnalare immediatamente al CSITEM o al Referente Informatico di struttura ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza;
- l'utente è tenuto a mantenersi aggiornato, controllando periodicamente le direttive del CSITEM.

A titolo esemplificativo e non esaustivo, è vietato:

1. accedere alla Rete Dati di Ateneo per conseguire l'accesso non autorizzato a risorse di rete interne od esterne all'Università; fornire il servizio di connettività di rete a soggetti non autorizzati all'accesso alla Rete d'Università;
2. usare false identità, l'anonimato o servirsi di risorse che consentono di restare anonimi; il CSITEM si riserva la facoltà di impedire in qualsiasi momento l'accesso alla Rete d'Università da parte di utenti anonimi o non sufficientemente identificati o identificabili;
3. violare gli obblighi in materia di copyright, licenze d'uso di software;
4. svolgere attività che causino malfunzionamento, diminuiscano la regolare operatività, danneggino o restringano l'utilizzabilità o le prestazioni della Rete dati di Ateneo. È altresì vietato manomettere in qualsiasi modo le apparecchiature e le strutture informatiche ed elettroniche dell'Ateneo;
5. violare la sicurezza di archivi e banche dati, compiere trasferimenti non autorizzati di informazioni

(software, basi dati, ecc.), intercettare, tentare d'intercettare o accedere a dati in transito sulla Rete Dati d'Ateneo, dei quali non si è destinatari specifici;
6. compiere azioni in violazione delle norme a tutela delle opere dell'ingegno, del diritto d'autore e del software;
7. distruggere o tentare di distruggere, danneggiare o tentare di danneggiare, intercettare o tentare di intercettare o accedere o tentare di accedere senza autorizzazione alla posta elettronica o ai dati di altri utenti o di terzi, usare, intercettare o diffondere o tentare di intercettare o diffondere password o codici d'accesso o chiavi crittografiche di altri utenti o di terzi, e in generale commettere o tentare di commettere attività che violino la riservatezza di altri utenti o di terzi, così come tutelata dalle norme civili, penali e amministrative applicabili;
8. diffondere immagini, dati o altro materiale potenzialmente offensivo, diffamatorio, o dal contenuto osceno;
9. utilizzare la Rete dati di Ateneo e i servizi da essa offerti a scopi commerciali e per propaganda politica o elettorale;
10. trasferire materiale in violazione delle norme sulla proprietà intellettuale, mediante programmi di tipo "Peer to Peer";
11. è vietato installare modem senza la preventiva autorizzazione del SISRA;
12. è vietato l'accesso ai locali e ai box riservati alle apparecchiature di rete, o apportare qualsiasi modifica agli stessi senza l'autorizzazione del SISRA;
13. è vietato cablare o collegare apparecchiature alle prese di rete senza l'autorizzazione del SISRA;
14. è vietato connettere un Host, contemporaneamente, alla rete d'Ateneo e ad altra rete (es. ADSL, GPRS) senza l'autorizzazione del SISRA;
15. è vietato copiare (a meno che la licenza d'uso non lo consenta) e/o utilizzare i programmi messi a disposizione dall'Amministrazione per installazioni esterne;
16. è vietato installare sui personal computer di proprietà dell'Amministrazione qualunque tipo di software e di hardware, anche se dotato di licenza d'uso, senza il previo assenso del SISRA, che verificherà preventivamente le caratteristiche del prodotto e le eventuali ripercussioni che una sua installazione potrebbe avere sul buon funzionamento della singola postazione o dell'intera rete.

Articolo 8

Modalità per l'erogazione di servizi

Premesso quanto già precisato nell'Articolo 1, ossia che la Rete Dati e le apparecchiature informatiche possono essere utilizzate esclusivamente per gli scopi autorizzati dal presente Regolamento, i soggetti autorizzati ad accedere alla Rete dati di Ateneo, possono erogare tramite essa dei servizi. Tali servizi dovranno essere conformi al presente regolamento ed ai regolamenti emanati dal GARR e dovranno essere autorizzati dal CSITEM.
Il CSITEM può bloccare o limitare temporaneamente l'erogazione di tali servizi da parte di un Host di rete, al fine di preservare il buon funzionamento della Rete Dati di Ateneo nella sua globalità.

Articolo 9

Ruolo del Coordinamento Servizi Informatici, Telematici e Multimediali (CSITEM)

L'Università degli Studi del Molise, per la finalità di cui all'Art.1 ha affidato al CSITEM la gestione tecnica della Rete dati di Ateneo**,** dei servizi informatici, telematici e multimediali dell'Ateneo.

Il Settore SISRA assicura in modo esclusivo il monitoraggio, l'aggiornamento ed ampliamento della Rete dati di Ateneo (cablaggio e parte attiva) sia sotto l'aspetto fisico che logico, curandone i relativi progetti.
Il SISRA nell'espletamento delle proprie attività di gestione e monitoraggio della Rete di Ateneo è:

1) titolare del trattamento dei dati di log relativi alle attività di rete dei singoli host (flussi generati, richieste DNS, indirizzi IP, servizi erogati sulla rete);
2) ha la facoltà di revocare temporaneamente le credenziali di accesso ai servizi e/o l'autorizzazione di accesso alla Rete Dati di Ateneo da parte di un Host di rete, o limitare la fruizione di servizi da parte dello stesso, a fronte di:
   - violazioni del presente regolamento o della normativa vigente applicabile;
   - di erogazione di servizi potenzialmente dannosi per un buon funzionamento delle Rete dati di Ateneo nel suo complesso;
3) ha la facoltà di bloccare la consultazione di siti WEB, Newsgroups e altre risorse nei casi di violazioni del presente regolamento o della normativa vigente.

Al SISRA è demandata la gestione sistemistica dei server finalizzati alla condivisione di risorse, degli accessi, dei servizi internet (www, mail, ftp, news) per tutta l'utenza (studenti, personale docente, e tecnico-amministrativo).
Inoltre ha la gestione tecnico-informatica dei servizi di Segreteria Studenti, Sistema Bibliotecario d'Ateneo, Contabilità Integrata d'Ateneo, Carriere e Stipendi, Protocollo, Presenze, Controllo Accessi, e tutti quei servizi le cui procedure, realizzate anche nella struttura, sono connessi a quelli precedentemente elencati.
Il SISRA gestisce il servizio di assistenza tecnico-funzionale di tutti gli apparati informatici dell'Università attraverso la procedura on-line "Servizio di Supporto ed Assistenza".

Al Settore SIM sono demandati:
- la gestione dei Laboratori Informatici e Linguistici dell'Ateneo attraverso il controllo del corretto funzionamento delle apparati informatici, il servizio di assistenza all'utenza, il controllo degli accessi nonché delle attività svolte da parte degli utenti;
- la gestione delle attività multimediali consistente nella realizzazione di produzioni e post-produzione audio-video, assistenza nelle iniziative istituzionali dell'Università (convegni, seminari, ecc.), videoconferenza;
- la gestione del Sito Web d'Ateneo;
- il supporto tecnico all'acquisto di tutti gli apparati informatici necessari alle esigenze infrastrutturali e dell'utenza dell'Ateneo.

Il PPSS si dedica alla programmazione, alla progettazione e sviluppo attività e servizi strategici inerenti l'informatica, alla gestione PoP e rete GARR, alla Formazione ed E-Learning, alla progettazione di nuove Infrastrutture e reti VoiP, alla gestione del Test Center ECDL. Supporta le attività di ricerca scientifica dell'Ateneo e la gestione, di tipo specialistico, dei server e delle infrastrutture di Rete.

Articolo 10

Referenti informatici di struttura

Per ogni struttura decentrata d'Ateneo deve essere nominato un Referente informatico.

I Referenti informatici di struttura rappresentano l’interfaccia amministrativa e tecnica dell’utenza verso il CSITEM.

I Referenti informatici di struttura devono operare secondo le direttive e le procedure stabilite dal CSITEM e nel rispetto delle norme previste dal presente regolamento, garantendone altresì il rispetto, per quanto di propria competenza, da parte dell’utenza gestita ed adottando tempestivamente i provvedimenti previsti.

I Referenti informatici di struttura devono curare la diffusione, all’interno dell’utenza gestita, delle notizie informative, delle procedure e note organizzative comunicate a tale scopo dal CSITEM, informando ed aggiornando inoltre tale utenza sulle funzioni proprie del Referente informatico di struttura. A tale scopo, essi devono consultare regolarmente la propria casella di posta elettronica sul dominio unimol.it, che verrà usata per la diffusione delle informazioni.

I Referenti informatici di struttura devono curare la distribuzione e/o installazione, nel rispetto delle norme amministrative e tecniche, stabilite caso per caso, dei software licenziati centralmente dal CSITEM e collaborano all’assistenza tecnico-funzionale degli apparati informatici relativi alla propria struttura.

I Referenti informatici di struttura devono conoscere l’organizzazione fisica della porzione di rete a servizio della propria struttura e devono collaborare con i responsabili e/o gestori degli Host in Rete e dei Servizi della porzione di rete di propria competenza.

Nei casi in cui la situazione logistica lo renda conveniente, i Referenti informatici di struttura possono essere incaricati di eseguire, solamente su specifica richiesta del CSITEM, le operazioni di gestione ordinaria sugli armadi che ospitano le apparecchiature di rete a servizio della propria struttura. In nessun caso i Referenti informatici dovranno intervenire sulle apparecchiature di rete e sul cablaggio strutturato di propria iniziativa.

Articolo 11
Protezione dei dati personali

L’Università tutela il diritto alla riservatezza relativo alle comunicazioni supportate dalla Rete Dati di Ateneo e ai dati personali presenti nella Rete stessa, in conformità alle norme legislative e regolamentari vigenti e applicabili.

In conformità a dette norme, gli Organi competenti dell’Ateneo possono monitorare i dati presenti nella Rete dell’Università, nelle circostanze previste dalle norme legislative e regolamentari vigenti e applicabili.

Il CSITEM custodisce per esigenze tecniche e per eventuale difesa di un diritto in sede giudiziaria, secondo gli usi e gli scopi consentiti dalla Legge e dai Regolamenti dell’Ateneo, i dati (log) relativi ai collegamenti e alle attività effettuati dagli utenti sulla rete, per un periodo di conservazione, come da normativa.

Articolo 12
Utilizzo dei Nomi a Dominio

Il dominio DNS unimol.it e tutti i sottodomini sono gestiti dal CSITEM nell’interesse dell'Ateneo.

Articolo 13
Aule informatiche

Le norme contenute nel presente regolamento si applicano anche alle aule informatiche e multimediali dell'Università degli Studi del Molise.

Il referente tecnico addetto all'aula disciplinerà l'accesso alle aule e l'uso delle apparecchiature informatiche assegnate.

Articolo 14
Variazione del Regolamento

L'Università degli Studi del Molise ha la facoltà di apportare modifiche e integrazioni al presente regolamento. Tali modifiche avverranno su proposta del CSITEM e dovranno essere approvate dagli Organi competenti.

Tutti gli utenti verranno informati delle modifiche. Il nuovo regolamento entrerà in vigore senza che vi sia l'obbligo di richiedere nuovamente l'accettazione da parte dell'utente.

Articolo 15
Violazioni

Il CSITEM può disattivare in qualsiasi momento un codice d'accesso personale e/o una password, disconnettere un Host in Rete, senza necessità di preventivo avviso, qualora la disattivazione sia necessaria all'integrità o al funzionamento della Rete Dati di Ateneo, oppure qualora vi sia fondato sospetto che l'Utente abbia violato il presente Regolamento.

Il CSITEM ha la facoltà di informare gli Organi competenti dell'Ateneo a fronte di comportamenti in violazione del presente regolamento o vi sia il fondato sospetto che ciò sia avvenuto.
La revoca permanente dell'autorizzazione di accesso alla Rete Dati di Ateneo, da parte di uno o più Host di Rete, dovrà essere disposta dal Dirigente su proposta del CSITEM.

Sono fatte salve le ulteriori conseguenze di natura penale, civile, amministrativa e disciplinare della violazione compiuta. In particolare, si rammenta che i comportamenti illeciti che integrano gli estremi di reati informatici ed elettronici, sono perseguibili dall'autorità giudiziaria e puniti a norma della legge penale.

ALLEGATO A - Acceptable Use Policy del GARR

1. La Rete Italiana dell'Università e della Ricerca Scientifica, denominata comunemente “la rete del GARR”, si fonda su progetti di collaborazione scientifica ed accademica tra le Università e gli Enti di Ricerca pubblici italiani. Di conseguenza il servizio di rete GARR è destinato principalmente alla comunità che afferisce al Ministero dell'Università e della Ricerca Scientifica e Tecnologica (MURST). Esiste tuttavia la possibilità di estensione del servizio stesso anche ad altre realtà che svolgono attività di ricerca in Italia, specialmente ma non esclusivamente in caso di organismi "no-profit" impegnati in collaborazioni con la comunità afferente al MURST. L'utilizzo della rete è comunque soggetto al rispetto delle Acceptable Use Policy (AUP) da parte di tutti gli utenti GARR.

2. Il “Servizio di rete GARR”, definito brevemente in seguito come “Rete GARR”, è costituito dall'insieme dei servizi di collegamento telematico, dei servizi di gestione della rete, dei servizi applicativi e di tutti quelli strumenti di interoperabilità (operati direttamente o per conto del GARR) che permettono ai soggetti autorizzati ad accedere alla rete di comunicare tra di loro (rete GARR nazionale).

Costituiscono parte integrante della rete GARR anche i collegamenti e servizi telematici che permettono la interconnessione tra la rete GARR nazionale e le altre reti.

3. Sulla rete GARR non sono ammesse le seguenti attività:

o fornire a soggetti non autorizzati all'accesso alla rete GARR il servizio di connettività di rete o altri servizi che la includono, quali la fornitura di servizi di housing, di hosting e simili, nonchè permettere il transito di dati e/o informazioni sulla rete GARR tra due soggetti entrambi non autorizzati all'accesso sulla rete GARR (third party routing);

o utilizzare servizi o risorse di rete, collegare apparecchiature o servizi o software alla rete, diffondere virus, hoaxes o altri programmi in un modo che danneggi, molesti o perturbi le attività di altre persone, utenti o i servizi disponibili sulla rete GARR e su quelle ad essa collegate;

o creare o trasmettere (se non per scopi di ricerca o comunque propriamente in modo controllato e legale) qualunque immagine, dato o altro materiale offensivo, diffamatorio, osceno, indecente, o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza o il credo;

o trasmettere materiale commerciale e/o pubblicitario non richiesto ("spamming"), nonchè permettere che le proprie risorse siano utilizzate da terzi per questa attività;

o danneggiare, distruggere, cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti, compresa l'intercettazione o la diffusione di parole di accesso (password) e chiavi crittografiche riservate;

o svolgere sulla rete GARR ogni altra attività vietata dalla Legge dello Stato, dalla normativa Internazionale, nonchè dai regolamenti e dalle consuetudini (“Netiquette”) di utilizzo delle reti e dei servizi di rete acceduti.

4. La responsabilità del contenuto dei materiali prodotti e diffusi attraverso la rete è delle persone che li producono e diffondono.

5. I soggetti autorizzati (S.A.) all'accesso alla rete GARR, definititi nel documento “Regole approvate dalla CRCS”, possono utilizzare la rete per tutte le proprie attività istituzionali. Si intendono come attività

istituzionali tutte quelle inerenti allo svolgimento dei compiti previsti dallo statuto di un soggetto autorizzato, comprese le attività all'interno di convenzioni o accordi approvati dai rispettivi organi competenti, purchè l'utilizzo sia a fini istituzionali.

Rientrano in particolare nelle attività istituzionali, la attività di ricerca, la didattica, le funzioni amministrative dei soggetti e tra i soggetti autorizzati all'accesso e le attività di ricerca per conto terzi, con esclusione di tutti i casi esplicitamente non ammessi dal presente documento.

Altri soggetti, autorizzati ad un accesso temporaneo alla rete (S.A.T.) potranno svolgere solo l'insieme delle attività indicate nell'autorizzazione.

Il giudizio finale sulla ammissibilità di una attività sulla rete GARR resta prerogativa degli Organismi Direttivi del GARR.

6. Tutti gli utenti a cui vengono forniti accessi alla rete GARR devono essere riconosciuti ed identificabili. Devono perciò essere attuate tutte le misure che impediscano l'accesso a utenti non identificati. Di norma gli utenti devono essere dipendenti del soggetto autorizzato, anche temporaneamente, all'accesso alla rete GARR.

Per quanto riguarda i soggetti autorizzati all'accesso alla rete GARR (S.A.) gli utenti possono essere anche persone temporaneamente autorizzati da questi in virtù di un rapporto di lavoro a fini istituzionali. Sono utenti ammessi gli studenti regolarmente iscritti ad un corso presso un soggetto autorizzato con accesso alla rete GARR.

7. È responsabilità dei soggetti autorizzati all'accesso, anche temporaneo, alla rete GARR di adottare tutte le azioni ragionevoli per assicurare la conformità delle proprie norme con quelle qui esposte e per assicurare che non avvengano utilizzi non ammessi della rete GARR. Ogni soggetto con accesso alla rete GARR deve inoltre portare a conoscenza dei propri utenti (con i mezzi che riterrà opportuni) le norme contenute in questo documento.

8. I soggetti autorizzati all'accesso, anche temporaneo, alla rete GARR accettano esplicitamente che i loro nominativi (nome dell'Ente, Ragione Sociale o equivalente) vengano inseriti in un annuario elettronico mantenuto a cura degli Organismi Direttivi GARR.

9. In caso di accertata inosservanza di queste norme di utilizzo della rete, gli Organismi Direttivi GARR prenderanno le opportune misure, necessarie al ripristino del corretto funzionamento della rete, compresa la sospensione temporanea o definitiva dell'accesso alla rete GARR stessa.

10. L'accesso alla rete GARR è condizionato all'accettazione integrale delle norme contenute in questo documento.

Emanato con D.R. n.1970 del 22 dicembre 2008